

file



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/458,921	12/10/1999	MOHAMMAD PEYRAVIAN	P-4541.001	9480

7590 10/23/2003
IBM CORPORATION DEPT T81/062
3039 CORNWALLS ROAD
RTP, NC 27709

EXAMINER

VAUGHAN, MICHAEL R

ART UNIT PAPER NUMBER

2131

DATE MAILED: 10/23/2003

5

Please find below and/or attached an Office communication concerning this application or proceeding.

Art Unit: 2131

Detailed Action

Claims 1-44 have been examined and are pending.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 12/10/99 was filed. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 15 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention as disclosed in the specification. Claim 15 outlines a method in which:

- d. encrypting the secret key with a second secret key to generate a key message;
- e. generating a second message authentication code based on said first message authentication code and said first secret key using a said second secret key;

The disclosure on page 14 reads that the generating of a second message authentication code uses a secret symmetric key, K_{MAC} . The disclosure on page 14 reads that a secret master key, K_M , encrypts the first secret key. From claim 15, it is unclear whether "said second secret key" refers to K_{MAC} or K_M . For purposes of this action, the examiner is assuming that the second secret key in step (e) is a secret master key.

Claim 15 also has the steps ordered incorrectly. There are two step f's and two step g's as labeled. The examiner is assuming this as a typo to maintain continuity but a correction is needed.

Art Unit: 2131

Claim 15 recites the limitation "said first secret key" in step e. There is insufficient antecedent basis for this limitation in the claim.

Claim Objections

A series of singular dependent claims is permissible in which a dependent claim refers to a preceding claim which, in turn, refers to another preceding claim.

A claim, which depends from a dependent claim, should not be separated by any claim which does not also depend from said dependent claim. It should be kept in mind that a dependent claim may refer to any preceding independent claim. In general, applicant's sequence will not be changed. See MPEP § 608.01(n).

Claim 34 depends on claim 23 but is included with claims dependent upon 29. The examiner is assuming claim 34 depends on claim 29 for the merits. A correction is necessary.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-14, 29-36, and 41-44 are rejected under 35 U.S.C. 102(b) as being anticipated by Haber et al (USP Re. 34,954).

As per claim 1, Haber et al teach:

Receiving a time stamp request at an outside agency at a first time, said time stamp request including identifying data associated with said document (column 2, line 55—column 3, line 10);

Art Unit: 2131

Creating at said outside agency a time stamp receipt based on said identifying data and a time indication (column 2, line 55—column 3, line 10);

Generating at said outside agency a message authentication code based on said time stamp receipt and a secret key (column 2, line 55—column 3, line 10 and column 4, lines 8-39);

Transmitting said time stamp receipt and said message authentication code to a designated party (FIG. 1, block 19);

Receiving a certification request at said outside agency at a second time, said certification request including said time stamp receipt and said message authentication code [57];

Validating said message authentication code at said outside agency using said secret key [57];

Certifying said time stamp receipt at said outside agency using a cryptographic signature scheme if said message authentication code is valid [57].

As per claims 2-6, Haber et al teach a method of identifying data that comprises a hash value generated from a one-way hash function and including the hash value and the time indication to the time stamp receipt (column 3, lines 10-65).

As per claim 7, Haber et al teach said time stamp request further includes an identification number associated with the requestor (column 3, lines 10-65 column 4, lines 8-39).

As per claim 8, Haber et al teach said message authentication code comprise a digital sequence generated by application of a deterministic function to said time stamp receipt and said secret key concatenate together (column 3, lines 10-65).

As per claim 9, Haber et al teach the step of validating said message authentication code includes recomputing said message authentication code at said outside agency using said received time stamp receipt and said secret key and comparing the recomputed message authentication code to said received message authentication code [57].

As per claim 10, Haber et al teach wherein the certifying step includes signing said message authentication code using a private signature key controlled by said outside agency [57].

As per claim 11, Haber et al teach wherein the certifying step includes signing said time stamp receipt using a private signature key controlled by said outside agency [57].

Art Unit: 2131

As per claim 12, Haber et al teach storing said secret key in a database at said outside agency (column 3, line 40-45). Having to remember the original number or secret key is necessary to validate one-way hash functions or MACs, which are one-way hash functions, which use a secret key. It is therefore inherent that the secret key is stored in a database where it can later be retrieved to certify a timestamp.

As per claim 13, Haber et al teach wherein each time stamp receipt includes a sequential record number that is used at said outside agency to look up said secret key in said database (column 4, lines 8-20).

As per claim 14, Haber et al teach the step of transmitting said certified time stamp receipt to said requestor (column 4, line 8-26).

As per claim 29, Haber et al teach:

Receiving a time stamp request at an outside agency at a first time, said time stamp request including identifying data associated with said document (column 2, line 55—column 3, line 10);

Creating at said outside agency a time stamp receipt based on said identifying data and a time indication (column 2, line 55—column 3, line 10);

Generating at said outside agency a message authentication code based on said time stamp receipt and a secret key (column 2, line 55—column 3, line 10 and column 4, lines 8-39);

Transmitting said time stamp receipt and said message authentication code to a designated party (FIG. 1, block 19).

As per claims 30-34, Haber et al teach a method of identifying data that comprises a hash value generated from a one-way hash function and including the hash value and the time indication to the time stamp receipt (column 3, lines 10-65).

As per claim 35, Haber et al teach said time stamp request further includes an identification number associated with the requestor (column 3, lines 10-65 column 4, lines 8-39).

Art Unit: 2131

As per claim 36, Haber et al teach said message authentication code comprise a digital sequence generated by application of a deterministic function to said time stamp receipt and said secret key concatenate together (column 3, lines 10-65).

As per claim 41, Haber et al teach:

Receiving a certification request at said outside agency at a second time, said certification request including said time stamp receipt and said message authentication code [57];

Validating said message authentication code at said outside agency using said secret key [57];

Certifying said time stamp receipt at said outside agency using a cryptographic signature scheme if said message authentication code is valid [57].

As per claim 42, Haber et al teach wherein the certifying step includes signing said message authentication code using a private signature key controlled by said outside agency [57].

As per claim 43, Haber et al teach wherein the certifying step includes signing said time stamp receipt using a private signature key controlled by said outside agency [57].

As per claim 44, Haber et al teach the step of transmitting said certified time stamp receipt to said requestor (column 4, line 8-26).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 15-28 and 37-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Haber et al in view of Doyle (WO 99/16209).

Art Unit: 2131

As per claims 15, 37-40 Haber et al teach:

Receiving a time stamp request at an outside agency at a first time, said time stamp request including identifying data associated with said document (column 2, line 55—column 3, line 10);

Creating at said outside agency a time stamp receipt based on said identifying data and a time indication (column 2, line 55—column 3, line 10);

Generating at said outside agency a message authentication code based on said time stamp receipt and a secret key (column 2, line 55—column 3, line 10 and column 4, lines 8-39).

Haber et al are silent in disclosing encrypting the secret key with a second secret key to generate a key message. Doyle teaches encrypting a public key with a secret private key [claim 8]. Encrypting a key with a private key creates a key message, which can be validated by a public key to prove authenticity. Also this procedure removes the agency from having to remember the first private key.

In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Doyle within the system of Haber et al because it would allow the first encryption key to be encrypted with the private key of the trusted agency prevent the agency from having to remember many private keys.

Haber et al are silent in disclosing generating a second message authentication code based on the first message authentication code. Doyle teaches encrypting data associated with the certification request using the second private key [pg. 12, lines 25-26 and claim 10]. Using the private key to encrypt data, attributes the encryption to a particular author whereby the data can be validated using the public key of the owner of the private key. It would have been obvious to one of ordinary skill that the first message authentication code can be validated by using the second secret key from the teaching of Doyle (pg. 11, line 30—pg. 12, line 1).

In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Doyle within the system of Haber et al because it would allow a second message authentication code to be created based on the first message authentication code which corresponds to a particular entity without having to remember both the first private key used and who it belongs to. Simply knowing the master private key is enough information to decrypt the message

Art Unit: 2131

authentication code to reveal who the owner of the data is and when it was signed without revealing the plaintext. Using the private key to encrypt data, attributes the encryption to a particular author whereby the data can be validated using the public key of the owner of the private key.

From the employing of the teachings of Doyle within the system of Haber et al, it follows that: Haber et al are silent in expressly disclosing transmitting a second message authentication code and the encrypted key message. The examiner supplies the same rationale for the motivation to incorporate the teachings of Doyle within the system of Haber et al. Therefore it would have been obvious to include the second message authentication code and the encrypted key message along with the time stamp receipt and first message authentication code to the requestor as Haber et al teach (column 2, line 55—column 3, line 10 and column 4, lines 8-39).

Haber et al teach validating the first message authentication code using said first secret key [57].

Haber et al teach certifying said time stamp receipt at said outside agency using a cryptographic signature scheme if said message authentication code is valid [57].

As per claims 16-20, Haber et al teach a method of identifying data that comprises a hash value generated from a one-way hash function and including the hash value and the time indication to the time stamp receipt (column 3, lines 10-65).

As per claim 21, Haber et al teach said time stamp request further includes an identification number associated with the requestor (column 3, lines 10-65 column 4, lines 8-39).

As per claim 22, Haber et al teach said message authentication code comprise a digital sequence generated by application of a deterministic function to said time stamp receipt and said secret key concatenate together (column 3, lines 10-65).

As per claim 23, the examiner supplies the same rationale for the motivation as recited in the rejection of claim 15 to incorporate the teachings of Doyle within the system of Haber et al to include a second message authentication code. Haber et al teach said message authentication code comprise a

Art Unit: 2131

digital sequence generated by application of a deterministic function to said time stamp receipt and said secret key concatenate together (column 3, lines 10-65). Therefore it would have been obvious that the second message authentication code also comprises a numeric representation.

As per claim 24, the examiner supplies the same rationale for the motivation as recited in the rejection of claim 15 to incorporate the teachings of Doyle within the system of Haber et al to include a second message authentication code. Haber et al teach the step of validating said message authentication code includes recomputing said message authentication code at said outside agency using said received time stamp receipt and said secret key and comparing the recomputed message authentication code to said received message authentication code [57]. It is obvious that, because the second message authentication code comprises that concatenation of the first message authentication code and the secret keys, that the first message authentication code which was sent would be compared to the first authentication code which is a part of the second message authentication code.

As per claim 25, Haber et al teach the step of validating said message authentication code includes recomputing said message authentication code at said outside agency using said received time stamp receipt and said secret key and comparing the recomputed message authentication code to said received message authentication code [57].

As per claim 26, Haber et al teach wherein the certifying step includes signing said message authentication code using a private signature key controlled by said outside agency [57].

As per claim 27, Haber et al teach wherein the certifying step includes signing said time stamp receipt using a private signature key controlled by said outside agency [57].

As per claim 28, Haber et al teach the step of transmitting said certified time stamp receipt to said requestor (column 4, line 8-26).

Art Unit: 2131

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent 5,778,071 Caputo et al.

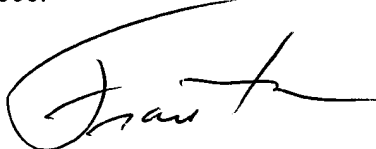
Menezes, Alfred, et al, Handbook of Applied Cryptography, pgs. 30-31, 455-459, CRC Press,
Washington D.C., 1996

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

MV
Michael R Vaughan
Examiner
Art Unit 2131


**FRANTZ B. JEAN
PRIMARY EXAMINER**